

A tighter bound for the number of words of minimum length in an automorphic orbit

Donghi Lee

Department of Mathematics, Pusan National University, Jangjeon-Dong, Geumjung-Gu, Pusan 609-735, South Korea

Received 31 October 2005

Available online 5 June 2006

Communicated by Efim Zelmanov

Abstract

Let u be a cyclic word in a free group F_n of finite rank n that has the minimum length over all cyclic words in its automorphic orbit, and let $N(u)$ be the cardinality of the set $\{v: |v| = |u| \text{ and } v = \phi(u) \text{ for some } \phi \in \text{Aut } F_n\}$. In this paper, we prove that $N(u)$ is bounded by a polynomial function of degree $2n - 3$ in $|u|$ under the hypothesis that if two letters x, y with $x \neq y^{\pm 1}$ occur in u , then the total number of $x^{\pm 1}$ occurring in u is not equal to the total number of $y^{\pm 1}$ occurring in u . We also prove that $2n - 3$ is the sharp bound for the degree of polynomials bounding $N(u)$. As a special case, we deal with $N(u)$ in F_2 under the same hypothesis.

© 2006 Elsevier Inc. All rights reserved.

1. Introduction

Let F_n be the free group of a finite rank n on the set $\{x_1, x_2, \dots, x_n\}$. We denote by Σ the set of letters of F_n , that is, $\Sigma = \{x_1, x_2, \dots, x_n\}^{\pm 1}$. As in [1,6], we define a *cyclic word* to be a cyclically ordered set of letters with no pair of inverses adjacent. The *length* $|w|$ of a cyclic word w is the number of elements in the cyclically ordered set. For a cyclic word w in F_n , we denote the automorphic orbit $\{\psi(w): \psi \in \text{Aut } F_n\}$ by $\text{Orb}_{\text{Aut } F_n}(w)$.

The purpose of this paper is to present a partial solution of the following conjecture proposed by Myasnikov and Shpilrain [7]:

E-mail address: donghi@pusan.ac.kr.

Conjecture. Let u be a cyclic word in F_n which has the minimum length over all cyclic words in its automorphic orbit $\text{Orb}_{\text{Aut } F_n}(u)$, and let $N(u)$ be the cardinality of the set $\{v \in \text{Orb}_{\text{Aut } F_n}(u) : |v| = |u|\}$. Then $N(u)$ is bounded by a polynomial function of degree $2n - 3$ in $|u|$.

This conjecture was motivated by the complexity of Whitehead's algorithm which decides whether, for given two elements in F_n , there is an automorphism of F_n that takes one element to the other. Indeed, proving that $N(u)$ is bounded by a polynomial function in $|u|$ would yield that Whitehead's algorithm terminates in polynomial time with respect to the maximum length of the two words in question (see [7, Proposition 3.1]).

Proposing this conjecture, Myasnikov and Shpilrain [7] proved that $N(u)$ is bounded by a polynomial in $|u|$ in F_2 . Later, Khan [3] improved their result by showing that $N(u)$ has the sharp bound of $8|u| - 40$ for $|u| \geq 9$ in F_2 , by which the conjecture was settled in the affirmative for F_2 . For a free group of bigger rank, Kapovich, Schupp, Shpilrain [2] showed that $N(u)$ is bounded by a constant depending only on n for u contained in an exponentially generic subset of F_n , and the author [4] recently proved that $N(u)$ is bounded by a polynomial function of degree $n(5n - 7)/2$ in $|u|$ under the following

Hypothesis 1.1.

- (i) A cyclic word u has the minimum length over all cyclic words in its automorphic orbit $\text{Orb}_{\text{Aut } F_n}(u)$.
- (ii) If two letters x_i (or x_i^{-1}) and x_j (or x_j^{-1}) with $i < j$ occur in u , then the total number of $x_i^{\pm 1}$ occurring in u is strictly less than the total number of $x_j^{\pm 1}$ occurring in u .

In the present paper, we prove under the same hypothesis that $N(u)$ is bounded by a polynomial function of degree $2n - 3$ in $|u|$, and that $2n - 3$ is the sharp bound for the degree of polynomials bounding $N(u)$:

Theorem 1.2. Let u be a cyclic word in F_n that satisfies Hypothesis 1.1. Then $N(u)$ is bounded by a polynomial function of degree $2n - 3$ in $|u|$.

Theorem 1.3. Let $n \geq 2$ be arbitrary. Then there exist a polynomial $p_n(t)$ of degree exactly $2n - 3$ in t and a sequence (u_l) of cyclic words in F_n satisfying Hypothesis 1.1 such that $|u_l| \rightarrow \infty$ as $l \rightarrow \infty$ and such that $N(u_l) \geq p_n(|u_l|)$. Thus $2n - 3$ is a sharp bound for the degree of a polynomial in $|u|$ bounding $N(u)$ from above, provided u is a cyclic word in F_n that satisfies Hypothesis 1.1.

As a special case, we deal with $N(u)$ in F_2 :

Theorem 1.4. Let u be a cyclic word in F_2 that satisfies Hypothesis 1.1. Then $N(u) \leq 8|u| - 40$. Moreover, there exists a sequence (u_l) of cyclic words in F_2 satisfying Hypothesis 1.1 such that $|u_l| \geq 9$, $|u_l| \rightarrow \infty$ as $l \rightarrow \infty$ and such that $N(u_l) = 8|u_l| - 40$. Thus $N(u)$ has the sharp bound of $8|u| - 40$ for $|u| \geq 9$.

The same technique as used in [4] is applied to the proofs of these theorems. The proofs will appear in Sections 3–5. In Section 2, we will establish a couple of technical lemmas which play an important role in the proof of Theorem 1.2.

Now we would like to recall several definitions. As in [4], a *Whitehead automorphism* σ of F_n is defined to be an automorphism of one of the following two types (cf. [5,8]):

(W1) σ permutes elements in Σ .

(W2) σ is defined by a set $A \subset \Sigma$ and a letter $a \in \Sigma$ with both $a, a^{-1} \notin A$ in such a way that if $x \in \Sigma$ then

(a) $\sigma(x) = xa$ provided $x \in A$ and $x^{-1} \notin A$;

(b) $\sigma(x) = a^{-1}xa$ provided both $x, x^{-1} \in A$;

(c) $\sigma(x) = x$ provided both $x, x^{-1} \notin A$.

If σ is of type (W2), we write $\sigma = (A, a)$. By (\bar{A}, a^{-1}) , we mean a Whitehead automorphism $(\Sigma - A - a^{\pm 1}, a^{-1})$. It is then easy to see that $(A, a)(w) = (\bar{A}, a^{-1})(w)$ for any cyclic word w in F_n .

We also recall the definition of the degree of a Whitehead automorphism of the second type (see [4]):

Definition 1.5. Let $\sigma = (A, a)$ be a Whitehead automorphism of F_n of the second type. Put $A' = \{i: \text{either } x_i \in A \text{ or } x_i^{-1} \in A, \text{ but not both}\}$. Then the *degree* of σ is defined to be $\max A'$. If $A' = \emptyset$, then the *degree* of σ is defined to be zero.

Let w be a fixed cyclic word in F_n that satisfies Hypothesis 1.1(i). For two letters $x, y \in \Sigma$, we say that x *depends on* y with respect to w if, for every Whitehead automorphism (A, a) of F_n such that

$$a \notin \{x^{\pm 1}, y^{\pm 1}\}, \quad \{y^{\pm 1}\} \cap A \neq \emptyset, \quad \text{and} \quad \exists v \in \text{Orb}_{\text{Aut } F_n}(w): \quad |(A, a)(v)| = |v| = |w|,$$

we have $\{x^{\pm 1}\} \subseteq A$. Then, as shown in [4], if x depends on y with respect to w , then y depends on x with respect to w .

We then construct the *dependence graph* Γ_w of w as follows: Take the vertex set as Σ , and connect two distinct vertices $x, y \in \Sigma$ by a non-oriented edge if either $y = x^{-1}$ or y depends on x with respect to w . Let C_i be the connected component of Γ_w containing x_i . Clearly there exists a unique factorization

$$w = v_1 v_2 \cdots v_t \quad (\text{without cancellation}),$$

where each v_i is a non-empty (non-cyclic) word consisting of letters in C_{j_i} with $C_{j_i} \neq C_{j_{i+1}}$ ($i \bmod t$). The subword v_i is called a C_{j_i} -*syllable* of w . By the C_k -*syllable length* of w denoted by $|w|_{C_k}$, we mean the total number of C_k -syllables of w . We also define $|w|_s$ as $|w|_s = \sum_{k=1}^n |w|_{C_k}$.

Example 1.6. Consider the cyclic word $u = x_1^2 x_2^3 x_3^4 x_4^5$ in F_4 . Letting $v = (\{x_2^{\pm 1}\}, x_1)(u) = x_1 x_2^3 x_1 x_3^4 x_4^5$, v is an automorphic image of u with $|v| = |u|$ (hence $\Gamma_u = \Gamma_v$). This implies that both $x_3^{\pm 1}$ and $x_4^{\pm 1}$ do not depend on $x_2^{\pm 1}$. Also putting $v' = (\{x_2^{\pm 1}\}, x_3^{-1})(u)$, we have $|v'| = |u|$, so that $x_1^{\pm 1}$ does not depend on $x_2^{\pm 1}$. Hence the connected component C_2 of Γ_u containing x_2 consists of only $x_2^{\pm 1}$. This way we can show that the dependence graph $\Gamma_u = \Gamma_v$ has four distinct connected components, each C_i of which contains only $x_i^{\pm 1}$. Thus $|u|_{C_i} = 1$ for each $1 \leq i \leq 4$ and so $|u|_s = 4$, whereas $|v|_{C_1} = 2$, $|v|_{C_j} = 1$ for each $2 \leq j \leq 4$ and so $|v|_s = 5$.

Example 1.7. Consider the cyclic word $u = x_1^2 x_2^3 x_3^2 x_4 x_3^{-1} x_4 x_3 x_4^3$ in F_4 , of which the dependence graph Γ_u has three distinct connected components $C_1, C_2, C_3 = C_4$. Putting $v = (\{x_2^{\pm 1}\}, x_3^{-1})^2(u) = x_1^2 x_3^2 x_2^3 x_4 x_3^{-1} x_4 x_3 x_4^3$, v is an automorphic image of u with $|v| = |u|$, so $\Gamma_u = \Gamma_v$. While $|u|_{C_i} = 1$ for each $1 \leq i \leq 4$ and so $|u|_s = 4$, $|v|_{C_1} = |v|_{C_2} = 1$, $|v|_{C_3} = |v|_{C_4} = 2$ and so $|v|_s = 6$.

2. Preliminary lemmas

Throughout this section, when we say that $\sigma = (A, a)$ is a Whitehead automorphism of F_n of degree i , the following restriction is additionally imposed:

$$a = x_j^{\pm 1} \quad \text{with } j > i.$$

For two automorphisms ϕ and ψ of F_n , by writing $\phi \equiv \psi$ we mean the equality of ϕ and ψ over all cyclic words in F_n , that is, $\phi(v) = \psi(v)$ for any cyclic word v in F_n . For a cyclic word v in F_n , we define $M_k(v)$, for $k = 0, 1, \dots, n-1$, to be the cardinality of the set $\Omega_k(v) = \{\phi(v) : \phi \text{ can be represented as a composition } \phi = \alpha_t \cdots \alpha_1 \text{ } (t \in \mathbb{N}) \text{ of Whitehead automorphisms } \alpha_i \text{ of } F_n \text{ of the second type such that } k = \deg \alpha_t \geq \deg \alpha_{t-1} \geq \cdots \geq \deg \alpha_1 \text{ and } |\alpha_i \cdots \alpha_1(v)| = |v| \text{ for all } i = 1, \dots, t\}$.

Lemma 2.1. *Under the foregoing notation, $M_1(v)$ is bounded by a polynomial function of degree $n-1$ in $|v|$.*

Proof. Let ℓ_i be the number of occurrences of $x_i^{\pm 1}$ in v for $i = 1, \dots, n$. Clearly

$$M_1(v) \leq M_1(x_1^{2\ell_2} x_2^{\ell_2} \cdots x_{n-1}^{\ell_{n-1}} x_n^{\ell_n + \ell_1 - 2}).$$

So it is enough to prove that $M_1(x_1^{2\ell_2} x_2^{\ell_2} \cdots x_{n-1}^{\ell_{n-1}} x_n^{\ell_n + \ell_1 - 2})$ is bounded by a polynomial function in $|v|$ of degree $n-1$. Noting that $|x_1^{2\ell_2} x_2^{\ell_2} \cdots x_{n-1}^{\ell_{n-1}} x_n^{\ell_n + \ell_1 - 2}|_s = n$, put

$$\Lambda = \{v' : |v'|_s = n \text{ and } v' \in \Omega_0(x_1^{2\ell_2} x_2^{\ell_2} \cdots x_{n-1}^{\ell_{n-1}} x_n^{\ell_n + \ell_1 - 2})\}.$$

Obviously the cardinality of the set Λ is $(n-1)!$.

Let $w \in \Omega_1(x_1^{2\ell_2} x_2^{\ell_2} \cdots x_{n-1}^{\ell_{n-1}} x_n^{\ell_n + \ell_1 - 2})$. Then for an appropriate $v' \in \Lambda$, there exist Whitehead automorphisms σ_i of degree 0 and τ_j of degree 1 such that

$$w = \tau_q \cdots \tau_1 \sigma_p \cdots \sigma_1(v'), \quad (2.1)$$

where $|\sigma_i \cdots \sigma_1(v')| = |v'|$ and $|\sigma_i \cdots \sigma_1(v')|_s \geq |\sigma_{i-1} \cdots \sigma_1(v')|_s$ for all $1 \leq i \leq p$, and $|\tau_j \cdots \tau_1 \sigma_p \cdots \sigma_1(v')| = |v'|$ for all $1 \leq j \leq q$. Here, the same reasoning as in [4, Lemma 4.1] shows that $\sigma_i \sigma_{i'} \equiv \sigma_{i'} \sigma_i$ for all $1 \leq i, i' \leq p$. Furthermore, the chain $\tau_q \cdots \tau_1$ in (2.1) can be chosen so that, for $\tau_{ij} = (A_{ij}, a_{ij})$,

$$\tau_q \cdots \tau_1 = (\tau_{qr} \cdots \tau_{r1}) \cdots (\tau_{2q_2} \cdots \tau_{21})(\tau_{1q_1} \cdots \tau_{11}), \quad (2.2)$$

where $A_{ij} = A_{ij'}$ for all $1 \leq j, j' \leq q_i$, and $x_1 \in A_{i1} \subsetneq A_{i+11}$.

We may assume without loss of generality that the index r in (2.2) is minimum over all chains satisfying (2.1) and (2.2). Clearly in (2.1)–(2.2) the element v' in Λ , the Whitehead automorphisms $\sigma_1, \dots, \sigma_p$, and the index r are determined by w ; so we put

$$v'_w = v', \quad \psi_w = \sigma_p \cdots \sigma_1, \quad \text{and} \quad r_w = r.$$

It is easy to see that r_w is at most $n - 1$.

For $s = 1, \dots, n - 1$, put

$$L_s = \text{the cardinality of the set } \{\psi_w(v'_w) : w \in \Omega_1(x_1^2 x_2^{\ell_2} \cdots x_{n-1}^{\ell_{n-1}} x_n^{\ell_n + \ell_1 - 2}) \text{ with } r_w = s\}.$$

Then in view of (2.1)–(2.2), we have

$$M_1(x_1^2 x_2^{\ell_2} \cdots x_{n-1}^{\ell_{n-1}} x_n^{\ell_n + \ell_1 - 2}) \leq 2^{(n-1)} |v| L_1 + 2^{2(n-1)} |v|^2 L_2 + \cdots + 2^{(n-1)^2} |v|^{n-1} L_{n-1},$$

since the number of possible A_{ij} 's and the indices q_i 's in (2.2) are less than or equal to 2^{n-1} and $|v|$, respectively. Hence it is enough to prove that each L_s is bounded by a polynomial function in $|v|$ of degree $n - s - 1$. Due to the result of [4, Lemma 4.1], there is nothing to prove for $s = 1$. So let $s \geq 2$ and put $E_i = A_{i1} - A_{i-11}$ for $i = 2, \dots, s$. This can possibly happen only when $\psi_w = \sigma_p \cdots \sigma_1$ in (2.1) can be re-arranged so that, for $\sigma_j = (B_j, b_j)$,

$$\psi_w = (\sigma_{t_{s+1}} \cdots \sigma_{t_s+1}) \cdots (\sigma_{t_2} \cdots \sigma_2) \sigma_1, \quad (2.3)$$

where $b_1 \in \{x_1^{\pm 1}\}$, $b_j^{\pm 1} \in E_i$ and either $B_j \subseteq E_i$ or $B_j \cap E_i = \emptyset$ provided $t_{i-1} < j \leq t_i$ ($t_1 = 1$), and $b_j^{\pm 1} \notin (\bigcup_{i=2}^s E_i + x_1^{\pm 1})$ and either $B_j \subseteq (\bigcup_{i=2}^s E_i + x_1^{\pm 1})$ or $B_j \cap (\bigcup_{i=2}^s E_i + x_1^{\pm 1}) = \emptyset$ provided $t_s < j \leq t_{s+1}$.

Now, for $i = 2, \dots, s$, let

$$h_i \text{ be the half of the cardinality of the set } E_i.$$

Put $h = \sum_{i=2}^s h_i$. It then follows from the result of [4, Lemma 4.1] that the number of cyclic words obtained by $\sigma_{t_{j+1}} \cdots \sigma_{t_j+1}$ applied to $(\sigma_{t_j} \cdots \sigma_{t_{j-1}+1}) \cdots (\sigma_{t_2} \cdots \sigma_2) \sigma_1(v'_w)$ is bounded by $|v|^{h_{j+1}-1}$ provided $j = 1, \dots, s - 1$ and by $|v|^{n-(h+1)-1}$ provided $j = s$. Moreover, the number of cyclic words derived from σ_1 applied to v'_w is bounded by $n - 2$. Therefore we have from (2.3) that

$$L_s \leq (n-1)!(n-2)|v|^{h_2-1} \cdots |v|^{h_s-1} |v|^{n-h-2} = (n-1)!(n-2)|v|^{n-s-1},$$

which is a polynomial function in $|v|$ of degree $n - s - 1$, as required. \square

Remark. The proof of Lemma 2.1 can be applied without further change if we replace consideration of a single cyclic word v , the length $|v|$ of v , and the total number of occurrences of $x_j^{\pm 1}$ in v by consideration of a finite sequence (v_1, \dots, v_m) of cyclic words, the sum $\sum_{i=1}^m |v_i|$ of the lengths of v_1, \dots, v_m , and the total number of occurrences of $x_j^{\pm 1}$ in (v_1, \dots, v_m) , respectively.

Lemma 2.2. Under the foregoing notation, for each $k = 2, \dots, n - 1$, $M_k(v)$ is bounded by a polynomial function of degree $n + k - 2$ in $|v|$.

Proof. Let ℓ_i be the number of occurrences of $x_i^{\pm 1}$ in v for $i = 1, \dots, n$. Since

$$M_k(v) \leq M_k(x_1^2 \cdots x_k^2 x_{k+1}^{\ell_{k+1}} \cdots x_{n-1}^{\ell_{n-1}} x_n^{\ell_n + \ell_1 + \cdots + \ell_{k-2k}}),$$

it suffices to show that $M_k(x_1^2 \cdots x_k^2 x_{k+1}^{\ell_{k+1}} \cdots x_{n-1}^{\ell_{n-1}} x_n^{\ell_n + \ell_1 + \cdots + \ell_{k-2k}})$ is bounded by a polynomial function in $|v|$ of degree $n + k - 2$. As in the proof of Lemma 2.1, put $\Lambda = \{v': |v'|_s = n \text{ and } v' \in \Omega_0(x_1^2 \cdots x_k^2 x_{k+1}^{\ell_{k+1}} \cdots x_{n-1}^{\ell_{n-1}} x_n^{\ell_n + \ell_1 + \cdots + \ell_{k-2k}})\}$.

Let $w \in \Omega_k(x_1^2 \cdots x_k^2 x_{k+1}^{\ell_{k+1}} \cdots x_{n-1}^{\ell_{n-1}} x_n^{\ell_n + \ell_1 + \cdots + \ell_{k-2k}})$. Then for an appropriate $v' \in \Lambda$, there exist Whitehead automorphisms γ_i of F_n such that

$$w = \gamma_q \cdots \gamma_{p+1} \gamma_p \cdots \gamma_1(v'), \quad (2.4)$$

where the length of v' is constant throughout the chain on the right-hand side, $\deg \gamma_i = 0$ provided $1 \leq i \leq p$, $\deg \gamma_i > 0$ provided $p < i \leq q$, and $|\gamma_j \cdots \gamma_1(v')|_s \geq |\gamma_{j-1} \cdots \gamma_1(v')|_s$ for all $1 \leq j \leq p$. Here, since $\gamma_i \gamma_{i'} = \gamma_{i'} \gamma_i$ for all $1 \leq i, i' \leq p$ by the same reasoning as in [4, Lemma 4.1], we may assume that either none of γ_i for $1 \leq i \leq p$ has multiplier x_1 or x_1^{-1} or only γ_1 has multiplier x_1 or x_1^{-1} . So (2.4) can be re-written as

$$w = \gamma_q \cdots \gamma_{p+1} \gamma_p \cdots \gamma_1 \gamma_0(v'),$$

where γ_0 is either the identity or a Whitehead automorphism of F_n of degree 0 with multiplier x_1 or x_1^{-1} , and none of γ_j for $1 \leq j \leq q$ has multiplier x_1 or x_1^{-1} .

Write

$$\gamma_0(v') = x_1 u_1 x_1 u_2 \quad \text{without cancellation.} \quad (2.5)$$

(Note that u_1 and u_2 are non-cyclic subwords in $\{x_2, \dots, x_n\}^{\pm 1}$.) Let F_{n+1} be the free group on the set $\{x_1, \dots, x_{n+1}\}$. From (2.5) we construct a pair (v_1, v_2) of cyclic words v_1, v_2 in F_{n+1} with $|v_1| + |v_2| = 2|v|$ as follows:

$$v_1 = x_1 u_1 x_{n+1} u_1^{-1} \quad \text{and} \quad v_2 = x_1 u_2 x_{n+1} u_2^{-1}.$$

For each $\gamma_j = (D_j, d_j)$ for $1 \leq j \leq q$, define a Whitehead automorphism ε_j of F_{n+1} as follows:

$$\begin{aligned} \text{if } x_1^{\pm 1} \in D_j, \quad & \text{then } \varepsilon_j = (D_j + x_{n+1}^{\pm 1}, d_j); \\ \text{if only } x_1 \in D_j, \quad & \text{then } \varepsilon_j = (D_j + x_1^{-1}, d_j); \\ \text{if only } x_1^{-1} \in D_j, \quad & \text{then } \varepsilon_j = (D_j - x_1^{-1} + x_{n+1}^{\pm 1}, d_j); \\ \text{if } x_1^{\pm 1} \notin D_j, \quad & \text{then } \varepsilon_j = (D_j, d_j). \end{aligned}$$

Then arguing as in the proof of [4, Lemma 4.2], we have $|\varepsilon_j \cdots \varepsilon_1(v_1)| + |\varepsilon_j \cdots \varepsilon_1(v_2)| = 2|v|$ for all $1 \leq j \leq q$. Moreover, by the construction of ε_j , ε_j is a Whitehead automorphism of F_{n+1} of degree at most k , and the defining set of ε_j contains either both of $x_1^{\pm 1}$ or none of $x_1^{\pm 1}$. This yields the same situation as for a chain of Whitehead automorphisms of F_{n+1} of maximum

degree $k - 1$. Hence by the induction hypothesis together with the remark after Lemma 2.1, $M_k(x_1^2 \cdots x_k^2 x_{k+1}^{\ell_{k+1}} \cdots x_{n-1}^{\ell_{n-1}} x_n^{\ell_n + \ell_1 + \cdots + \ell_k - 2k})$ is bounded by $(n - 2)$ times a polynomial function in $2|v|$ of degree $(n + 1) + (k - 1) - 2 = n + k - 2$, as required. \square

3. Proof of Theorem 1.2

Without loss of generality we may assume that u satisfies further:

- (i) The C_n -syllable length $|u|_{C_n}$ of u is minimum over all cyclic words in the set $\{v \in \text{Orb}_{\text{Aut } F_n}(u) : |v| = |u|\}$.
- (ii) If the index j ($1 \leq j \leq n - 1$) is such that $C_j \neq C_k$ for all $k > j$, then the C_j -syllable length $|u|_{C_j}$ of u is minimum over all cyclic words in the set $\{v \in \text{Orb}_{\text{Aut } F_n}(u) : |v| = |u| \text{ and } |v|_{C_k} = |u|_{C_k} \text{ for all } k > j\}$.

(Namely, we may assume that u satisfies further the conditions in [4, Hypothesis 1.3].) Let $u' \in \text{Orb}_{\text{Aut } F_n}(u)$ be such that $|u'| = |u|$. Due to the result of [4, Theorem 1.4], there exist Whitehead automorphisms π of the first type and τ_1, \dots, τ_s of the second type such that

$$u' = \pi \tau_s \cdots \tau_1(u),$$

where $n - 1 \geq \deg \tau_s \geq \deg \tau_{s-1} \geq \cdots \geq \deg \tau_1$, and $|\tau_i \cdots \tau_1(u)| = |u|$ for all $i = 1, \dots, s$. This implies that

$$N(u) \leq C(M_0(u) + M_1(u) + \cdots + M_{n-1}(u)), \quad (3.1)$$

where C is the number of Whitehead automorphisms of F_n of the first type (which depends only on n), and $M_k(u)$ is as defined in Section 2. The result of [4, Lemma 4.1] shows that $M_0(u)$ is bounded by a polynomial function in $|u|$ of degree $n - 2$. Also by Lemmas 2.1 and 2.2, $M_k(u)$ for each $k = 1, \dots, n - 1$ is bounded by a polynomial function in $|u|$ of degree $n + k - 2$. Then the required result follows from (3.1).

4. Proof of Theorem 1.3

In [7], Myasnikov and Shpilrain pointed out that experimental data provided by C. Sims show that the maximum value of $N(u)$ in F_3 is $48|u|^3 - 480|u|^2 + 1140|u| - 672$ if $|u| \geq 11$ and this maximum value is attained at $u = x_1^2 x_2^2 x_3 x_2^{-1} x_3 x_2 x_3^\ell$ with $\ell \geq 3$. Inspired by this observation, we let

$$u = x_1^2 x_2^2 (x_2 x_n x_2^{-1} x_n) x_2 x_3 (x_3 x_n x_3^{-1} x_n)^2 x_3 \cdots x_{n-1} (x_{n-1} x_n x_{n-1}^{-1} x_n)^{n-2} x_{n-1} x_n^\ell$$

with $\ell \gg 1$ in F_n . Note that u satisfies Hypothesis 1.1. For this u , we will prove that $N(u)$ cannot be bounded by a polynomial function in $|u|$ of degree less than $2n - 3$. For each $i = 2, \dots, n - 1$ and $j = 1, \dots, n - 1$, let

$$\sigma_i = (\{x_i^{\pm 1}, \dots, x_n^{\pm 1}\}, x_n^{-1}) \quad \text{and} \quad \tau_j = (\{x_j, x_{j+1}^{\pm 1}, \dots, x_{n-1}^{\pm 1}\}, x_n^{-1});$$

then σ_i and τ_j are Whitehead automorphisms of F_n of degree 0 and degree j , respectively. Then the total number of cyclic words derived from automorphisms of F_n of the form

$\tau_{n-1}^{m_{n-1}} \cdots \tau_1^{m_1} \sigma_{n-1}^{k_{n-1}} \cdots \sigma_2^{k_2}$, where $k_i, m_j \leq \frac{\ell}{2n-3}$, applied to u is $(\frac{\ell}{2n-3})^{2n-3}$. Hence $N(u)$ is at least $(\frac{\ell}{2n-3})^{2n-3}$, which completes the proof. \square

5. Proof of Theorem 1.4

Let us assume that u satisfies further:

- (i) The C_2 -syllable length $|u|_{C_2}$ of u is minimum over all cyclic words in the set $\{v \in \text{Orb}_{\text{Aut } F_n}(u) : |v| = |u|\}$.
- (ii) If $C_1 \neq C_2$, then the C_1 -syllable length $|u|_{C_1}$ of u is minimum over all cyclic words in the set $\{v \in \text{Orb}_{\text{Aut } F_n}(u) : |v| = |u| \text{ and } |v|_{C_2} = |u|_{C_2}\}$.

(Namely, assume that u satisfies further the conditions in [4, Hypothesis 1.3].) Note that $M_0(u) = 1$ in F_2 , where $M_0(u)$ is as defined in Section 2. Also every Whitehead automorphism of F_2 of degree 1 is equal to either $(\{x_1\}, x_2)$ or $(\{x_1\}, x_2^{-1})$ over all cyclic words in F_2 . Hence, in view of [4, Theorem 1.4], $N(u)$ is the same as the cardinality of the set $\{v : v = \pi \tau^k(u) \ (k \geq 0)\}$, where π is a permutation on Σ and τ is either $(\{x_1\}, x_2)$ or $(\{x_1\}, x_2^{-1})$ such that $|\tau^i(u)| = |u|$ for all $i = 1, \dots, k$. Let

$$\Lambda(u) = \{v : v = \tau^k(u) \ (k \geq 0), \text{ where } \tau \text{ is as above}\}.$$

Let m be the number of occurrences of $x_1^{\pm 1}$ in u . First consider the maximum value $N(u)$ over all u with $m = 2$. If $m = 2$, then u is of the form either $x_1 x_2^{\ell_1} x_1^{-1} x_2^{\ell_2}$ or $x_1^2 x_2^{\ell}$. Then the cardinality of $\Lambda(x_1 x_2^{\ell_1} x_1^{-1} x_2^{\ell_2})$ equals 1 and that of $\Lambda(x_1^2 x_2^{\ell})$ equals $|u| - 1$. Hence $N(u)$ has the maximum value at $u = x_1^2 x_2^{\ell}$. For $u = x_1^2 x_2^{\ell}$ with $\ell \geq 3$, $N(u) = 4(|u| - 1)$, since there are 8 permutations on Σ and $\tau^j(x_1^2 x_2^{\ell}) = \pi \tau^{\ell-j}(x_1^2 x_2^{\ell})$ for $j \geq \ell/2$, where $\tau = (\{x_1\}, x_2^{-1})$ and π is the permutation that fixes x_1 and maps x_2 to x_2^{-1} .

Next consider the maximum value of $N(u)$ over all u with $m = 4$. (Here note that if m is odd, then any Whitehead automorphism of degree 1 cannot be applied to u without increasing $|u|$; hence the cardinality of $\Lambda(u)$ equals 1.) It is not hard to see that $\Lambda(u)$ has the maximum cardinality $|u| - 5$ at $u = x_1^2 x_2 x_1^{-1} x_2 x_1 x_2^{\ell}$. For $u = x_1^2 x_2 x_1^{-1} x_2 x_1 x_2^{\ell}$ with $\ell \geq 3$, $N(u) = 8(|u| - 5)$, since 8 permutations on Σ applied to the elements of $\Lambda(x_1^2 x_2 x_1^{-1} x_2 x_1 x_2^{\ell})$ induce all different cyclic words. Obviously this is the maximum value of $N(u)$ over all u with $m = 4$.

Finally note that the cardinality of $\Lambda(u)$ cannot be greater than nor equal to $|u| - 5$ for any u with $m > 4$. This means that $N(u) < 8(|u| - 5)$ for every u with $m > 4$. Therefore, the maximum value of $N(u)$ over all u is $8(|u| - 5)$, which is attained at $u = x_1^2 x_2 x_1^{-1} x_2 x_1 x_2^{\ell}$ with $\ell \geq 3$.

Acknowledgments

The author is grateful to the referee for many helpful comments and suggestions. This work was supported by Pusan National University Research Grant, 2004.

References

- [1] P.J. Higgins, R.C. Lyndon, Equivalence of elements under automorphisms of a free group, J. London Math. Soc. 8 (1974) 254–258.

- [2] I. Kapovich, P.E. Schupp, V. Shpilrain, Generic properties of Whitehead's algorithm and isomorphism rigidity of random one-relator groups, *Pacific J. Math.* 223 (2006) 113–140.
- [3] B. Khan, The structure of automorphic conjugacy in the free group of rank two, in: *Computational and Experimental Group Theory*, in: *Contemp. Math.*, vol. 349, Amer. Math. Soc., Providence, RI, 2004, pp. 115–196.
- [4] D. Lee, Counting words of minimum length in an automorphic orbit, *J. Algebra* 301 (1) (2006) 35–58.
- [5] R.C. Lyndon, P.E. Schupp, *Combinatorial Group Theory*, Springer-Verlag, New York, 1977.
- [6] J. McCool, A presentation for the automorphism group of a free group of finite rank, *J. London Math. Soc.* 8 (1974) 259–266.
- [7] A.G. Myasnikov, V. Shpilrain, Automorphic orbits in free groups, *J. Algebra* 269 (2003) 18–27.
- [8] J.H.C. Whitehead, Equivalent sets of elements in a free group, *Ann. of Math.* 37 (1936) 782–800.